

EJK:LAL
F.#2012R00996

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

12 M 758

- - - - -X

IN THE MATTER OF AN APPLICATION FOR
A SEARCH WARRANT FOR:

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR A SEARCH
WARRANT

THE PREMISES KNOWN AND DESCRIBED AS
BLACKBERRY 9630, SERIAL NUMBER
305F141B; ZTE-G 6502, NON-FLIP
CELLULAR PHONE SERIAL NUMBER
32591241B973; AND MOTOROLA, NON-FLIP
CELLULAR PHONE SERIAL NUMBER
J32YLS6BV2

- - - - -X

EASTERN DISTRICT OF NEW YORK, SS:

Michael Martinez, being duly sworn, deposes and states that he is a Special Agent of the United States Department of Homeland Security, Homeland Security Investigations ("HSI"), duly appointed according to law and acting as such.

Upon information and belief, there is probable cause to believe that there is located in THE PREMISES KNOWN AND DESCRIBED AS BLACKBERRY 9630, SERIAL NUMBER 305F141B; ZTE-G 6502, NON-FLIP CELLULAR PHONE SERIAL NUMBER 32591241B973; and MOTOROLA, NON-FLIP CELLULAR PHONE SERIAL NUMBER J32YLS6BV2 (the "SUBJECT DEVICES"), further described in Attachment A, for the things described in Attachment B, which constitutes fruits, evidence and instrumentalities of a conspiracy to import and to distribute and

possess with the intent to distribute narcotics in violation of Title 21, United States Code, Sections 841(a)(1), 846, 952(a), 960 and 963. The source of your deponent's information and the grounds for his belief are as follows:¹

1. I am a Special Agent with HSI. I have been employed by the United States Department of Homeland Security for three years. I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for importation and possession of narcotics, including cocaine. I have participated in investigations involving search warrants and arrest warrants. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

2. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: my personal participation in this investigation, reports made to me by other law enforcement authorities, and review of other records and reports.

¹ Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned during the course of the investigation.

3. The United States Department of Homeland Security, HSI is investigating the unlawful importation of cocaine and possession of cocaine with the intent to distribute.

I. BACKGROUND

4. On or about June 22, 2012, Jean Rolen St. Surin ("St. Surin") arrived at John F. Kennedy International Airport ("JFK Airport") in Queens, New York, aboard American Airlines Flight No. 896, which originally departed from Port Au Prince, Haiti.

5. St. Surin was selected for a Customs and Border Protection ("CBP") examination. St. Surin presented for inspection one piece of luggage. St. Surin claimed ownership of the bag and its contents.

6. During an inspection of the bag, a CBP officer noticed that the bottom of the suitcase was unusually thick. The bottom of the suitcase was probed, revealing a white powdery substance, which field-tested positive for cocaine.

7. The total approximate gross weight of the cocaine found in St. Surin's suitcase is 3,795 grams. The white powdery substance was transported to the Drug Enforcement Administration Northeast Laboratory for analysis.

8. St. Surin was placed under arrest and was advised of his Miranda warnings, which he indicated he understood and agreed to waive. St. Surin indicated in sum and substance that

"MANO" was involved. At the time of his arrest, he had among his possessions the SUBJECT DEVICES.

9. On or about June 22, 2012, Pierre Marie Fourcand ("Fourcand") also arrived JFK Airport in Queens, New York, aboard the same American Airlines Flight No. 896, which originally departed from Port Au Prince, Haiti. Fourcand was selected for a Customs and Border Protection ("CBP") examination. Fourcand presented for inspection one piece of luggage which when probed, revealed a white powdery substance, which field-tested positive for cocaine. The drugs were concealed in the bottom of his luggage, the same location where St. Surin's drugs were found. Fourcand was placed under arrest and at the time of his arrest, he also had among his possessions three cellular telephones: a BLACKBERRY CURVE, SERIAL NUMBER A000001CE1E84D; SAMSUNG SCH-R380, NON-FLIP CELLULAR PHONE SERIAL NUMBER A000002AA4F830; AND SAMSUNG FLIP-PHONE SGH-A707, SERIAL NUMBER RVKP904145L.

10. A brief search of Fourcand's phones and observed a text message referencing a person named "MANNO." Fourcand was questioned about the phones and indicated that MANNO is a friend in Haiti.

11. Based on my training and experience there is probable cause to believe that Fourcand and St. Surin may have been sent to the United States by the same organization or

individuals since they had in their possession three similar cellular phones and they both referenced a person allegedly named "MANO" or MANNO."

II. TECHNICAL TERMS

12. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and

downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. Electronic mail: Electronic mail, commonly called email or e-mail, is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks. A sent or received email typically includes the content of the message, source and destination addresses, the date and time at which the email was sent, and the size and length of the email. If a sender or recipient of the message does not delete the message, the message can remain on the device indefinitely. If an email user writes a draft message but does not send it, that message may also be saved on the device but may not include all of these categories of data. The SUBJECT DEVICES can also store files, including emails, address books, contact or buddy lists, calendar data, pictures, and other files. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, emails on the device, and attachments to emails, including pictures and files.

e. Text Messages: Text messaging, or texting, refers to the exchange of brief written text messages between fixed-line phone or mobile phone and fixed or portable

devices over a network, and included messages which contain image, video, and sound content.

f. Facebook/MySpace: Facebook and MySpace are a social networking services and websites. Users of these sites may create a personal profile, add other users as friends, and exchange messages, including automatic notifications when they update their profile. Users must register before using the site. Users can create profiles with photos, lists of personal interests, contact information, and other personal information. Users can communicate with friends and other users through private or public messages and a chat feature. Users can access and store personal information, such as contacts, telephone numbers, and photographs on their accounts.

III. THE SUBJECT DEVICES

13. Based upon my knowledge, training, and experience, I know that those who import, distribute, and possess with intent to distribute narcotics often communicate by means of wireless telephones such as the SUBJECT DEVICES. Those who commit such offenses may also retain evidence of their participation in such crimes on wireless telephones through call records, text messages, emails, or photos. Based upon my

knowledge, training, and experience, I know that those who import, distribute, and possess with intent to distribute narcotics often communicate by means of text messages or electronic mail.

14. CBP recovered the SUBJECT DEVICES from St. Surin after finding cocaine in his luggage. Based upon my training and experience with cases involving drug couriers who arrive at the airport with narcotics concealed in their luggage, I know that drug couriers are commonly instructed to call someone upon their arrival to the United States to arrange delivery of the narcotics. Based upon my training and experience, I know that drug couriers often save, in their wireless telephones, contact information and directions concerning the delivery of the narcotics. Accordingly, there is probable cause to believe there is information stored on the SUBJECT DEVICES pertaining to calls to and from St. Surin, and contact information and numbers concerning St. Surin's importation of the cocaine on or about June 22, 2012.

15. Based on my training, experience, and research, I know that the SUBJECT DEVICES can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the SUBJECT DEVICES. This information can sometimes be recovered with forensic tools. Based upon my training and experience, I

know that instruments such as the SUBJECT DEVICES have capabilities that allow them to serve as wireless telephones and digital cameras, and can be used to send and receive electronic mail and text messages and to access the Internet and websites including Facebook and MySpace. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the SUBJECT DEVICES.

IV. TECHNICAL BACKGROUND

16. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the SUBJECT DEVICES because:

b. Data on an electronic device can provide evidence of a file that was once on the device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the device that show what tasks and processes were recently active. Web

browsers, email programs, and chat programs store configuration information on the device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the device was in use. Electronic devices can record information about the dates files were created and the sequence in which they were created.

c. Forensic evidence on an electronic device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the electronic device at a relevant time.

d. A person with appropriate familiarity with how an electronic device works can, after examining this

forensic evidence in its proper context, draw conclusions about how devices were used, the purpose of their use, who used them, and when.

e. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on an electronic device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, such evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the device and the application of knowledge about how the device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

f. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on an electronic device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

17. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.


18. Because this warrant seeks only permission to examine a devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a Device. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

V. CONCLUSION

19. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the SUBJECT DEVICES there exists evidence of crimes. Accordingly, a search warrant is requested.

20. WHEREFORE, your deponent respectfully requests that the requested search warrant be issued for THE PREMISES KNOWN AND DESCRIBED AS BLACKBERRY 9630, SERIAL NUMBER 305F141B; ZTE-G 6502,

NON-FLIP CELLULAR PHONE SERIAL NUMBER 32591241B973; and MOTOROLA,
NON-FLIP CELLULAR PHONE SERIAL NUMBER J32YLS6BV2.



Michael Martinez
Special Agent
Homeland Security Investigations

Sworn to
14 day

THE HONOR
UNITED ST
EASTERN D

SE

ATTACHMENT A

Property to Be Searched

The property to be searched is a BLACKBERRY 9630, SERIAL NUMBER 305F141B; ZTE-G 6502, NON-FLIP CELLULAR PHONE SERIAL NUMBER 32591241B973; and MOTOROLA, NON-FLIP CELLULAR PHONE SERIAL NUMBER J32YLS6BV2, hereinafter the "Subject Devices." This warrant authorizes the forensic examination of the Subject Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B
Particular Things to be Seized

All information obtained from the Subject Devices will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing all information described below that constitutes fruits, evidence and instrumentalities of a conspiracy to import and to distribute and possess with the intent to distribute narcotics in violation of Title 21, United States Code, Sections 841(a)(1), 846, 952(a), 960 and 963, including:

1. All records and information on the Subject Devices described in Attachment A, including names and telephone numbers, as well as the contents of all call logs, contact lists, text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Facebook posts, Internet activity (including browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits or instrumentalities of a conspiracy to import and to distribute and possess with the intent to distribute narcotics occurring on or about June 22, 2012, in violation of Title 21, United States Code, Sections 841(a)(1), 846, 952(a), 960 and 963.
2. Evidence of user attribution showing who used or owned the Subject Devices at the time the things described in this warrant were created, edited, or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;
3. Evidence of software that would allow others to control the Subject Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
4. Evidence of the lack of such malicious software;
5. Evidence of the attachment to the Subject Devices of other storage devices or similar containers for electronic evidence;
6. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Subject Devices;
7. Evidence of the times the Subject Devices were used;

8. Passwords, encryption keys, and other access devices that may be necessary to access the Subject Devices; and

9. Contextual information necessary to understand the evidence described in this attachment,

all of which constitute evidence, fruits and instrumentalities of a conspiracy to import and to distribute and possess with the intent to distribute narcotics in violation of Title 21, United States Code, Sections 841(a)(1), 846, 952(a), 960 and 963.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.